

## IT Security Day

Cyber Society of India

November 30, 2006

Address by Mr David T Hopper, Consul General of South India, Chennai

### **The Role of Cyber security in U.S.-India Trade and Technology Relationship**



When I saw the list of distinguished speakers preceding me at today's event I feared that after listening to them there would be little left for me to say. That may indeed be the case, but I will take advantage of your kind invitation to speak today and press ahead with a few comments.

There can be no doubt that one of the important components for the expanding trade and technology relationship between the United States and India is cyber security. *Cyber security involves the protection of information networks and computing assets. This includes (i) protecting sensitive information from unauthorized disclosure or interception, (ii) safeguarding the accuracy and completeness of information and software, and (iii) ensuring that information and vital services are available to users when required.*

Many observers call the era in which we live the "Information Age" because our economies and our security are dependent on information technology. *At the core of this global digital economy is the Internet, which is composed of millions of interconnected computer networks that power today's marketplace. Businesses and consumers use the Internet to gather information, to purchase goods and services, and to handle financial transactions. Indeed, the ubiquity of the Internet has forced companies to reconsider business models, adopt new technologies, and seek efficiencies by leveraging their use of the Internet. Governments also rely on information technology and the information infrastructure to facilitate the delivery of essential services to the public.*

While the Information Age has brought innovation, economic growth, and a higher quality of life, it has also spawned new and unique vulnerabilities. Computer systems and networks create new avenues for malicious actors – ranging from hackers and common criminals to foreign intelligence agencies and international terrorists – who can do damage to all of us. In an age when entire industries – such as telecommunications, banking and finance, transportation, and energy – rely on information technology, we are now vulnerable to cyber attacks and cyber terrorism, including viruses, malicious code, denial of services attacks, and identity theft.

In fact, while a cyber attack would not, of course, be considered a weapon of mass *destruction*, it can be thought of as a weapon of mass *disruption*. One person with relatively little training, inexpensive equipment, and access to the Internet has the potential to disable an entire network or infrastructure. The financial and other costs related to such attacks are enormous. Corporations are on the front lines of the Information Age, and they routinely face the threat of cyber attack.

The U.S. government recognizes the threat of these vulnerabilities to our economy and security, and has developed a national strategy to address them. In February 2003, the Bush Administration released its National Strategy to Secure Cyberspace, which seeks to marshal government and private sector resources to prevent cyber attacks on America's critical infrastructures, to reduce national vulnerability to such attacks, and to minimize damage and recovery time from attacks that do occur. The Administration identified five national priority areas for our government's attention: first, a national cyber security response system; second, a national cyberspace security threat and vulnerability reduction program; third, a national cyberspace security awareness and training program; fourth, securing government's cyberspace; and fifth, national security and international cyberspace security cooperation.

The last priority -- the need for international cooperation is worth dwelling on in this forum. International cooperation is essential because there are no boundaries in cyberspace. The vulnerabilities of the Information Age transcend national borders. Our information and communications infrastructures are converging into a seamless global network. This means that, as we transmit proprietary business data, sensitive personal information, and protected intellectual property back and forth between our countries, it is critical that we work

together to coordinate and implement cyber security strategies and policies. This is essential for the growth of the global digital economy.

### **U.S.-India Initiatives on Cyber security**

The United States welcomes India as a vital partner in addressing such global cyber security issues. Our two economies are becoming increasingly interconnected through the growth of computer software development in both countries, as well as the growing trend in utilizing information technology-related services in each other's country. The United States and India must work together to ensure a secure environment for information exchanges, commercial transactions, and software development.

In light of our growing interdependence in information technology, President Bush and then-Prime Minister Vajpayee agreed in November 2001 to establish the U.S.-India Cyber terrorism Initiative. Since that time, our two governments have worked closely to address cyber security issues. In April 2002, the two governments convened a meeting in New Delhi of the U.S.-India Cyber security Forum, and discussed ways to better coordinate joint cyber security activities regarding standards, legal and law enforcement issues, defense, and infrastructure protection.

Through this framework, the United States seeks to work with India to develop appropriate standards for cyber security and to strengthen national laws and enforcement capabilities. While we favor a regulatory approach that is not excessive or burdensome on legitimate businesses and consumers, we also believe it is important that national laws on cyber crime be harmonized, so that hackers and others do not move from country to country in search of lax enforcement and non-existent penalties.

### **The Public-Private Partnership**

Governments, of course, can only do so much, because so many of our information systems and networks are owned and operated by the private sector. Accordingly, the cornerstone of our national cyber security strategy, as well as our cyber security initiatives with India, is an effective partnership with industry. After all, industry is in the best position to identify threats and vulnerabilities, articulate the need for security and protection of assets, and share ideas and best practices

for the development of cyber security technologies, policies, and programs.

That is why I am delighted that programs such as today's are taking place and why I and the government I represent are pleased to be involved with them. The private sector has an important role in translating government initiatives into concrete joint activity at the business-to-business and people-to-people levels. While government can create the appropriate environment for commercial activity, it is up to private businesses, organizations, and individuals in both countries to reach out and build relationships. As part of this process, to truly unlock the potential of the U.S.-India trade and technology relationship, our governments and publics must work as partners to secure the information networks, systems, and infrastructures that drive the economic activity between our two countries.

Thank you.